Community of Shared Future：the Study on Global Network Security Model

Zhi Li
College of Media and Art
Ningbo Institute of Technology,Zhejiang University
Ningbo, China
lizhi@nit.zju.edu.cn

***Abstract*—With the widespread penetration of the Internet, cyberspace has now become the fifth space beyond land, sea, air, and the universe. Through the deep integration of virtual space and real world, more and more people are carrying social activities, while various known and unknown cyber security risks keep emerging, which has attracted global attention and even become the main topic of internet global governance. Then, how to find the key for a community of shared future in cyberspace is a common consensus in the international community. In particular, the "four principles" and "five propositions" advocated by President Xi Jinping at the world Internet conference have been widely recognized by the world. They respect cyber sovereignty, carry forward the spirit of partnership and cooperation, jointly safeguard and govern cyber security, and jointly build a community of shared future in cyberspace.**

Keywords—Community, Global Cyberspace Security, Model

I. ANALYSIS OF THE SITUATION OF GLOBAL NETWORK SECURITY

In recent years, information leakage has occurred frequently in the global network environment, and the scope and impact of information leakage have been escalating. According to the "Global Data Leakage Cost Study 2017" the global data reveal that cost research report, the total global 419 samples, the data reveal that the total cost of $14.1 billion on average, increased by 1.8% than normal size, whether government agency or organization enterprise, informatization level, the more developed countries, some large-scale data reveal that cause the more serious(IBM,2017). Its contents involve frequent exposure of private events such as payment information, harassment information, life and financial information. It can be seen that the losses caused by information leakage are not only limited to the economic aspect, but also involve personal privacy, and even have an impact on the stability of social order, which is very worrying to all countries in the world. Combined with the specific situation of global network security, it is mainly reflected in four aspects: cyber security threat, cyber war conflict, cyber terrorism and cyber hegemonism.

First, the threat of cyber security is increasingly serious, and the government's core departments are still the main targets of cyber attacks. At present, the number of global cyber attacks continues to increase, and the frequency of attacks is on the rise. Such as, international hacking organizations such as “Anonymous” and “Lulz Security” have been highly intrusive in recent years, often targeting government agencies, financial organizations, and health departments, including the invasion of the US CIA and Sony Corporation of Japan. Media tycoon Murdoch's TV station(Pei Tong,2018). As early as in the 2012 Global Risk World Economic Forum, cyber attacks by governments and commercial organizations have been included in one of the five major threats to global stability(Huanqiu,2018).

Secondly, cyber warfare has become an important part of modern warfare. From the national level analysis, the intention of preparing for "cyber warfare" became more and more obvious. The network security company McAfee released a research report in November 2009, "In the immediate future: the era of network wars." Large countries such as the United States and France are accumulating website weapons, smashing espionage activities, using the network to control wars, and guarding against the outbreak of cyber warfare(Cheng Gong,2014). Looking at the form of international cyber warfare, the United States is in a dominant position in cyber warfare because it controls most of the facilities of the global Internet, relying on strong hardware and software strength, and dare to start firstly.

Third, cyber terrorism has also spread, and the Internet has become the main battlefield for terrorists to declare war. Terrorist organizations use the Internet to collect a large amount of information from governments, use the Internet to collect money and get rid of the original mode of exchange and donation, and develop towards intelligence to obtain political, military and economic information about the country. In particular, the popularity of new media has set off a new wave of cyber terror and provided convenient conditions for cyber terrorism. In addition, since the outbreak of the "Prism Gate" incident in the United States, the global panic has confirmed that the United States has absolute control over information in the field of network information security. The formation of cyber hegemonism has prompted countries around the world to pay more attention to cybersecurity issues.

Therefore, the development of global cybersecurity is not optimistic, has evolved into a strategic issue of the world, and has stimulated the evolution of international social form and competition. Although more and more countries have raised their cybersecurity issues to the national strategic level, they are also fighting for the control of information in cyberspace, consolidating the right to develop cyberspace, protecting the privacy of Internet users, combating international cybercrime, and preventing cyberspace breaches. Other issues have started a series of discussions and collaborations, but the results are minimal.

  DOI: 10.25236/emcs.2018.083

However, fortunately, the construction of a global cyberspace community advocated by the Chinese government in recent years has received more and more attention and recognition from all over the world. It has launched a network security cooperation conference, established corresponding institutions, and strengthened network security construction. The foundation of the global cybersecurity destiny community has laid the foundation.

II. THE CONSTRUCTION OF A GLOBAL CYBERSECURITY DESTINY COMMUNITY

The construction of a global cybersecurity destiny community is a long process, and global cybersecurity issues have evolved into a level of governance. At present, the main body of the construction is diversified, including the state, social organizations, network media, opinion leaders, and netizens. The goal is to actively participate in the allocation of information resources, public opinion guidance, and order maintenance through effective participation of the main body, and effectively solve the network. Safely existing information imbalance, public opinion crisis, disorderly order, etc., jointly create freedom and equality in cyberspace, and thus continue to maintain a stable and healthy development network. The theoretical basis of the construction is based on the “Community of shared future for mankind” and based on the "five adherences" of China's new cosmopolitanism, and actively advocates a multilateral, democratic and transparent global network security governance system. Such as, We should oppose hegemonism and western centrism, and advocate a multipolar world and cultural diversity; We should oppose regional protectionism and advocate free circulation and open cooperation of people, money, goods and information; We should oppose egoism and advocate joint consultation, shared interests and common prosperity.;We should oppose interference in other countries' internal affairs, advocate harmony and inclusiveness, market operation and peaceful development; We should oppose denial, distortion and falsification of history, and advocate that history be kept in mind to prevent the recurrence of historical tragedies(Peiren Shao&Junwei Wang,2018). The foundation of the construction is that China has already adopted the concept of network security innovation governance, bridging the digital divide, carrying out multilateral international cooperation, and making positive contributions to the international rules and network governance mechanisms of global cyberspace security.

First, hold to the neo-cosmial theory and promote the construction of a global cybersecurity destiny community. Specifically, it protects the critical infrastructure and information security of the global network, maintains the order of the world's cyberspace, eliminates the digital divide, and advocates joint construction; We will Accelerate the pace of network facilities construction, encourage Internet technology innovation, and promote the sharing of global resources for the Internet; We will crack down on cybercrime and terrorist activities in accordance with the law, oppose cyber hegemonism, advocate the diversified development of global network culture, actively carry out international cooperation in cybersecurity, respect national sine sovereignty, protect personal privacy and intellectual property rights, realize global network governance, and guarantee human rights equality. So, the main body of cyberspace construction is a virtual space with multiple participations. It has become an indispensable part of human destiny. It advocates multi-polarization of the world, builds a multi-cooperative global network security governance mechanism, and promotes the network. The construction of a community of security destiny benefits mankind and has practical significance.

Secondly, maintaining the bottom line fairness, open cooperation, democratic participation, sovereign equality, legal order, and data security as the principles of global cyber security governance is a concrete manifestation of the "five adherences" in New Worldism. From the perspective of the global network security governance environment, the development of global networks requires an internationally recognized, government-first responsibility, social compensation, universal sharing, weak priority, and lasting effects of social regulation(Tiankui Jing,2013). With this open cooperation, create a relaxed development environment, build more collaborative platforms, and lay the foundation for the governance of network security. It emphasizes the democratic and equal attributes of the Internet, maintains the social order of cyberspace, and recognizes that data security is not only a part of the global network strategic resources, but also an inevitable requirement for the development of the big data era, and one of the principles of global cybersecurity.

Once again, bear in mind the global network “disaster”, avoid historical reenactment, clarify the real risks of the Internet, promote the establishment of a global network security governance mechanism, strengthen the four core layers of global network security, and finally form a concentric structure of global network security governance. The four core layers of global cybersecurity include the management of key technologies for the Internet and the standardization of technical standards; the integration of key Internet resources into the regulatory system, such as website domain names, server systems, etc.; monitoring and management of user behavior standards, such as networks Spam, cyber fraud, etc.; for the industry derived from the development of the Internet, sound management regulations, such as intellectual property rights, personal reputation rights. Of course, with the development of the Internet, the governance of global network security has gradually formed, including key resources management, network information security, network development and construction, free flow of information, intellectual property protection, and economic and trade(Guo feng,2012). it analyzes the real environment of global network security and divides the responsibilities and obligations of global cyber security actors. The main body of cyber behavior is composed of the Internet's audience - Internet users, Internet companies, Internet organizations, and Internet public power executors. As the main body of network behavior, in the process of global network security governance, it is mainly controlled by technical means, and the self-discipline of the network convention self-discipline, while still accepting the management of the state department and the supervision of the public. Although the Internet has spread to all corners of the world, its forms are diverse, such as public welfare organizations, groups, intergovernmental international organizations, non-governmental organizations, or regional associations, but so far, in addition to the Internet Convention and Outside the Internet Treaties, there is no globally recognized organization responsible for maintaining and managing the Internet. In the global network

environment, governments as the executors of Internet public power have the most network resources and strong network control. They have the responsibility to promote the improvement of the network environment and ensure the orderly participation of network actors. The contribution of cyber security. In addition, in the global network security governance, the government as the main body of network security behavior, in addition to promoting the renewal of network technology, is more obliged to prosper the development of network culture, maintain network information security, participate in the construction of global network values, and develop global network security. The standards of behavior, as well as the spatial order of the global network, aim at the community of cyber security destiny, advocate multi-agents, participate in a series of internal and external mechanisms, implement common maintenance and governance, ensure peaceful development, and share benefits.

III. CYBERSPACE DESTINY COMMUNITY SECURITY MODEL

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. Model Construction

Regardless of the effect of birth rate and mortality on the total number of people, the SIR model divides all individuals in the population into three categories, namely, S-infected, I-infected, and R-immunized. The parameter table of the dynamic differential equation is shown in Table I.

TABLE I. DYNAMIC DIFFERENTIAL EQUATION MODEL

Symbol	The meaning of a community of shared future in cyberspace SIR model
S	Poor information potential spread members, S' is the rate of propagation
I	I' is a member of bad information dissemination
R	Members who have been quarantined and supervised
a	Bad information transmission rate
b	The weight of bad information supervision (the time span of bad information from monitoring to management is t, b=1/t)

B. The Dynamic Differential Equation is

$$S^{\prime}=-a*S*I \tag{1}$$

$$I^{\prime}=a*S*I-b*I \tag{2}$$

$$R^{\prime}=b*I \tag{3}$$

C. Model Simulation Comparison

In this paper, Anaconda3 is used to simulate the established mathematical model. During the propagation process, members of the cyberspace fate community change, such as the joining and leaving of new members, and the relationship between nodes. Due to the relatively short time of bad communication, according to the current domestic public opinion monitoring method, this paper does not consider the dynamic changes of the network for the time being, that is, the community structure of the network space destiny of the propagation process remains unchanged and the total number of users remains unchanged.

According to the current domestic public opinion management measures, the daily supervision of each day (9:00-9:30, 4:30-5:00), from the discovery of bad information to the disposal management time of about 1.5 days, the weight of bad information supervision b =0.67, we set two sets of parameters for comparative analysis.

TABLE II COMPARISON GROUP 1

Symbol	1Group1	2Group2
a	1.5	1.5
b	0.67	0.47

In the case of the same bad information transmission rate a, the impact of different regulatory efficiency on the cyberspace destiny community is shown in table 1. When the regulatory weight is high, that is, the governance efficiency of the cyberspace destiny community is high, the number of bad information dissemination will be The lower the number of propagation nodes that need to be isolated or controlled is lower than the group 2, which means that improving the efficiency of governance can

effectively reduce the follow-up management expenditure of the regulatory authorities in the security level of the cyberspace fate community.

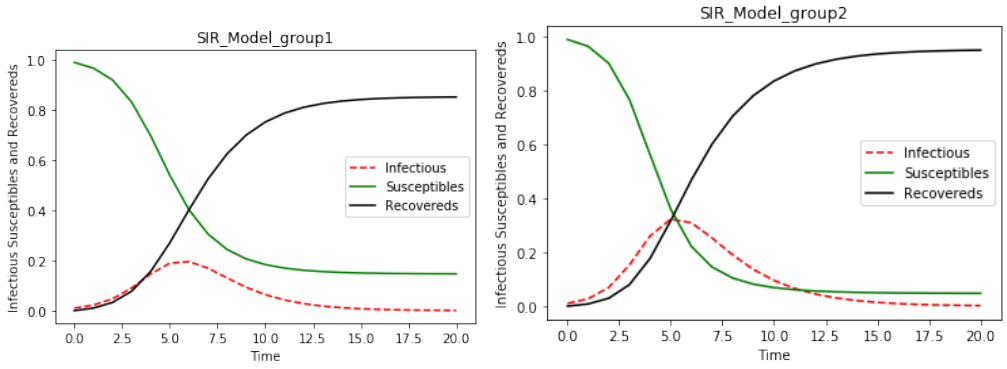

Fig.1

When the weight of bad information supervision is the same, if we improve the resistance of community members to bad information through education and other methods, and reduce the rate of transmission of bad information, we set two sets of parameters for comparison, as shown in Table III.

TABLE III COMPARISON GROUP 2

Symbol	1Group1	2Group2
a	1.0	1.5
b	0.67	0.67

In the case of the same regulatory efficiency b, the impact of different bad information transmission rates on the cyberspace destiny community is shown in table3. When the transmission rate is low, that is, the members of the cyberspace destiny community have strong immunity to bad information, bad information. The number of people transmitted will decrease, and the node that needs to be isolated or controlled will be lower than group 2.

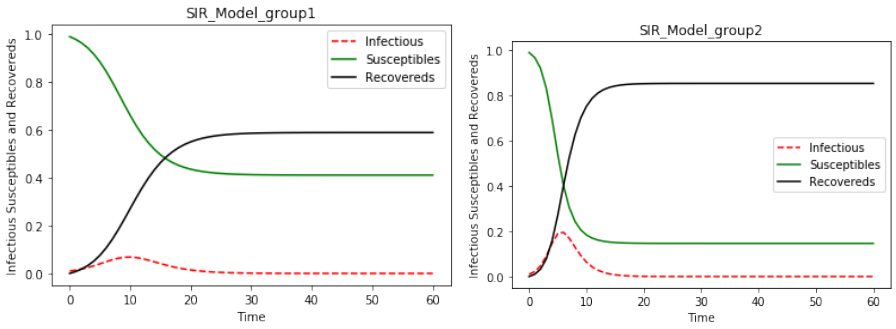

Fig.2

IV. CONCLUSION

The construction of a community of shared future in global cyberspace is a long process, How has global cyberspace been managed. At present, the main body of the construction is diversified, including the state, social organizations, online media, opinion leaders, and netizens. The goal is to actively participate in the allocation of information resources, public opinion guidance, and order maintenance through the active participation of the main body, effectively solve the problems of information imbalance, public opinion crisis, disorder of order, etc., and jointly create freedom and equality in cyberspace. Continue to maintain a stable and healthy development network. The theoretical basis of the construction is based on the "a community of shared future for human–" and based on the "five adherences" of China's new cosmopolitanism, and actively advocates a multilateral, democratic and transparent global network security governance system. That is, "persisting against hegemonism and Western centralism, advocating world multi-polarization and cultural pluralism; persisting in opposing regional protectionism, advocating free flow of people, money, goods and information, open cooperation; persisting in opposing self-interest and advocating for business Co-construction, win-win sharing, symbiosis and common prosperity; persist in opposing interference in other countries' internal affairs, advocate harmonious and inclusive, market operation, and peaceful development; persist in opposing denial, distortion, and tampering with history, and advocate keeping in mind history and preventing historical tragedies from repeating themselves(Peiren Shao, Junwei Wang,2018). The foundation of the construction is that China has already adopted the concept of network security innovation governance, bridging the digital divide, carrying

out multilateral international cooperation, and making positive contributions to the international rules and network governance mechanisms of global cyberspace security.

Hold to the new world theory and promote the establishment of a community of Shared future for global cyber security. Specifically, it protects the critical infrastructure and information security of the global network, maintains the order of the world's cyberspace, eliminates the digital divide, and advocates joint construction; Accelerate the pace of network facilities construction, encourage Internet technology innovation, and promote the sharing of global resources for the Internet. Fight against cybercrime and terrorist activities in accordance with the law, oppose cyber hegemonism, and advocate the diversified development of global network culture; Actively carry out international cooperation on cybersecurity, respect national sine sovereignty, protect personal privacy and intellectual property rights, achieve global network governance, and guarantee human rights equality. Therefore, the main body of the construction of cyberspace is a multivariate and jointly participated virtual space, which has become an indispensable part of the common destiny of mankind. Therefore, it is of practical significance to advocate a multi-polarization of the world, jointly build a multivariate and cooperative global network security governance mechanism, and promote the construction of a community of shared future in cyberspace to benefit mankind.

The principle that the bottom line is fair, open and cooperative, democratic participation, sovereign equality, legal order and data security are the principles of internet global security governance is a concrete manifestation of the "five tenets" of the new world doctrine. From the perspective of the internet global security governance environment, the development of global network needs a social regulation with international recognition, government first responsibility, social compensation, public sharing, priority of the weak and lasting effect(Tiankui Jing,2013). In this way, we will open up cooperation, create a loose development environment and build more cooperation platforms to lay the foundation for the governance of cyber security. It emphasizes the democratic and equal attributes of the Internet, maintains the social order of cyberspace, and recognizes that data security is not only a part of the global network strategic resources, but also an inevitable requirement for the development of the big data era, and one of the principles of global cyber security.

Bearing in mind the global network “disaster”, avoiding historical reenactment, clarifying the real risks of the Internet, promoting the establishment of a internet global security governance mechanism, strengthening the four core layers of global network security, and finally forming a concentric structure of internet global security governance. The four core layers of global cyber security are as follows: To manage and standardize the key technologies of the Internet; To Incorporate key resources of the Internet into the regulatory system, such as website domain names and server systems; To Conduct monitoring and management of user codes of conduct, such as network spam, network fraud, etc.; For the industries derived from the development of the Internet, sound management regulations, such as intellectual property rights and personal reputation rights. Of course, with the development of the Internet, the governance of global network security has gradually formed, including key resources management, network information security, network development and construction, free flow of information, intellectual property protection, and economic and trade(Guo Feng,2012).

REFERENCES

[1] Cheng Gong. Research on Foreign Network Information Security Strategy. Beijing: Publishing House of Electronics Industry Press. 2014,pp,35.

[2] Guo Feng. International Internet Governance Agency Research [D].Beijing: Beijing University of Posts and Telecommunications. 2012,pp,34.

[3] Huan Qiu. The world entered the era of "cyber cold war" and actively prepared for war with the United States and France. http://mil.huanqiu.com/world/2009-11/635937.html,2009-11-18/2018-06-25

[4] IBM Security.2017 Cost of Data Breach Study: Golbal Overview.Phonemon Institute Research Report,2017.

[5] Peiren Shao, Junwei Wang. Communication studies require neo-cosmial ideas and thinking.Journal of Education and Media Studies,2018, 2(13).

[6] Pei Tong. Us hackers have hit bottom, with an estimated cyber army of more than 100,000. http://news.cntv.cn/2013/03/29/ARTI1364547899827149.shtml, 2013-03-29/2018-06-28.

[7] Tiankui Jing. Bottom line fair welfare model.Beijing: China social sciences press.2013,pp,50.